How to check your email authentication in message headers

Whenever someone asks "why is my Mautic email going to spam?", the first thing to ask for is the headers of a test email. Nine times out of ten the answer is sitting in one line called Authentication-Results. This guide shows you how to find it and what it's telling you, so you can check SPF, DKIM and DMARC yourself in a couple of minutes.

The header is added by the mailbox provider that receives your email, and its format is defined in RFC 8601 (Kucherawy, 2019).

Step 1. Send yourself a test email

Send a Mautic email to mailboxes you control, ideally at Gmail, Outlook.com and Yahoo. Use a real marketing email if you can, sent the same way you send to contacts, so you're testing the real setup.

For a quick all-in-one check, you can also send a test to mail-tester.com. It gives you a score covering authentication, blocklists and content, which is a handy starting point before you dig into the headers.

Step 2. Open the message source

- **Gmail** Open the email, click the three dots, choose **Show original**. Gmail shows a handy summary of SPF, DKIM and DMARC at the top.
- **Outlook.com** Open the email, click the three dots, choose **View** then **View message source**.
- **Yahoo** Open the email, click the three dots, choose **View raw message**.

Search the source for Authentication-Results. Use the one nearest the top, which was added by the provider you're testing with. Ignore any further down, since anyone can add a fake one before sending.

Step 3. Read the results

A healthy Mautic email looks something like this.

```
Authentication-Results: mx.google.com;   dkim=pass header.i=@yourdoma
in.com header.s=mautic2026;   spf=pass smtp.mailfrom=bounce@mail.your
domain.com;   dmarc=pass (p=QUARANTINE) header.from=yourdomain.com
```

Check these four things.

Look for	What it tells you	What you want
dkim= and header.i or header.d	Whether DKIM passed, and which domain signed	pass, with your domain
spf= and smtp.mailfrom	Whether SPF passed, and for which return path	pass, with your domain or a subdomain
dmarc= and header.from	Whether DMARC passed for your From domain	pass
The policy in brackets after DMARC	Your current DMARC policy	What you expect to see

Step 4. Fix what you find

What you see	What it usually means	What to do
spf=pass but smtp.mailfrom is your provider's domain	SPF passes for them, not you	Set up a custom return path at your email service
spf=permerror	Your SPF record is broken	Check for two SPF records or more than ten lookups

dkim=pass but signed by your provider's domain	Signed, but not by you	Finish domain authentication at your email service
dkim=fail with "body hash did not verify"	Something changed the email after signing	Look for gateways adding footers or disclaimers
dkim=none	Not signed at all	Check the From address matches your authenticated domain
dmarc=fail even though SPF and DKIM pass	Neither passed for your From domain	Get DKIM signing with your own domain

Whenever someone asks "why is my Mautic email going to spam?", the first thing to ask for is the headers of a test email. Nine times out of ten the answer is sitting in one line called Authentication-Results. This guide shows you how to find it and what it's telling you, so you can check SPF, DKIM and DMARC yourself in a couple of minutes.

The header is added by the mailbox provider that receives your email, and its format is defined in RFC 8601 (Kucherawy, 2019).

Step 1. Send yourself a test email

Send a Mautic email to mailboxes you control, ideally at Gmail, Outlook.com and Yahoo. Use a real marketing email if you can, sent the same way you send to contacts, so you're testing the real setup.

For a quick all-in-one check, you can also send a test to mail-tester.com. It gives you a score covering authentication, blocklists and content, which is a handy starting point before you dig into the headers.

Step 2. Open the message source

- **Gmail** Open the email, click the three dots, choose **Show original**. Gmail shows a handy summary of SPF, DKIM and DMARC at the top.
- **Outlook.com** Open the email, click the three dots, choose **View** then **View message source**.
- **Yahoo** Open the email, click the three dots, choose **View raw message**.

Search the source for Authentication-Results. Use the one nearest the top, which was added by the provider you're testing with. Ignore any further down, since anyone can add a fake one before sending.

Step 3. Read the results

A healthy Mautic email looks something like this.

```
Authentication-Results: mx.google.com;   dkim=pass header.i=@yourdomain.com header.s=mautic2026;   spf=pass smtp.mailfrom=bounce@mail.yourdomain.com;   dmarc=pass (p=QUARANTINE) header.from=yourdomain.com
```

Check these four things.

Look for	What it tells you	What you want
dkim= and header.i or header.d	Whether DKIM passed, and which domain signed	pass, with your domain
spf= and smtp.mailfrom	Whether SPF passed, and for which return path	pass, with your domain or a subdomain
dmarc= and header.from	Whether DMARC passed for your From domain	pass
The policy in brackets after DMARC	Your current DMARC policy	What you expect to see

Step 4. Fix what you find

What you see	What it usually means	What to do
spf=pass but smtp.mailfrom is your provider's domain	SPF passes for them, not you	Set up a custom return path at your email service
spf=permerror	Your SPF record is broken	Check for two SPF records or more than ten lookups
dkim=pass but signed by your provider's domain	Signed, but not by you	Finish domain authentication at your email service

dkim=fail with "body hash did not verify"	Something changed the email after signing	Look for gateways adding footers or disclaimers
dkim=none	Not signed at all	Check the From address matches your authenticated domain
dmarc=fail even though SPF and DKIM pass	Neither passed for your From domain	Get DKIM signing with your own domain
dmarc=none	No DMARC record	Publish a _dmarc record

The detailed fixes are in *How to set up SPF for Mautic*, *How to set up DKIM for Mautic* and *How to set up DMARC for Mautic*.

Other headers worth a look

While you're in the source, check these too.

- **List-Unsubscribe and List-Unsubscribe-Post** should both be there on marketing email, see *How to set up one-click unsubscribe in Mautic*.
- **Return-Path** shows the bounce address. If it's not on your domain, that explains an unaligned SPF result.
- **ARC-Authentication-Results** appears when an email has been forwarded, and records what the forwarding server saw when it arrived. See "Why some of your own emails fail DMARC" in *How to set up DMARC for Mautic*.

Remember

A pass means your authentication works. It doesn't guarantee the inbox. Reputation, complaints and how engaged your contacts are still do a lot of the heavy lifting.

Over to you

What's the strangest thing you've found hiding in a set of email headers? I'd love to collect a few anonymised examples to add to this guide!

References

Kucherawy, M. (2019) *Message header field for indicating message authentication status*. RFC 8601. Internet Engineering Task Force. Available at https://www.rfc-editor.org/rfc/rfc8601 (Accessed 26 October 2026).

Online URL: https://kb.mautic.org/article/how-to-check-your-email-authentication-in-message-headers.html